JOURNAL OF NUMBER THEORY 25, 53–71 (1987)

Elliptic Units and a Kummer's Criterion for Imaginary Quadratic Fields

HIROSHI SAITO

College of General Education,
Kyoto University, Kyoto 606, Japan

Communicated by Y. Ihara

Received March 13, 1985

DEDICATED TO PROFESSOR MASAYOSHI NAGATA ON HIS 60TH BIRTHDAY

The article discusses a criterion for the existence of certain cyclic extensions of prime degree p of abelian extensions of imaginary quadratic fields. The condition in the criterion is given in terms of special values of L-functions with Grössencharacters. The method is based on the theory of elliptic units by Siegel, Ramachandra and Robert. © 1987 Academic Press, Inc.

INTRODUCTION

Recently, a Kummer's criterion for imaginary quadratic field was studied by several authors (cf. Coates and Wiles [1], Gillard [2], Hida [4], Robert [10], Yager [13]). In this paper, we will discuss it, following and developing the method of Robert, which is based on the theory of elliptic units.

Let K be an imaginary quadratic field. We denote by $\mathfrak{o}$ and h the ring of integers and the class number of K, respectively. For an integral ideal $\mathfrak{g}$, let $K(\mathfrak{g})$ (resp. $I(\mathfrak{g})$) be the maximal ray class field (resp. ray class group) modulo $\mathfrak{g}$. Let p be a prime number not dividing $6h$, and $\mathfrak{p}$ a prime divisor of p in K. We take an integral ideal $\mathfrak{f}_0$ prime to $\mathfrak{p}$. If p decomposes in K, we assume $\bar{\mathfrak{p}}$ divides $\mathfrak{f}_0$ at most once, where $\bar{\mathfrak{p}}$ is the conjugate of $\mathfrak{p}$ over $\mathbf{Q}$. There exists an elliptic curve E with $\mathrm{End}(E) = \mathfrak{o}$ defined over the Hilbert class field H of K, which has good reduction at all primes dividing $\mathfrak{p}\mathfrak{f}_0$. Let M be an abelian extension of K contained in $K(\mathfrak{f}_0)(E_\mathfrak{p})$, where $E_\mathfrak{p}$ is the group of $\mathfrak{p}$ division points of E. Assume $[M: K]$ is prime to p and M is not contained in $K(\mathfrak{f}_0)$. We shall give a criterion for the existence of cyclic extensions of M of degree p which satisfies certain conditions in terms of special values of L-functions of K with Grössencharacters (see Theorem 4.1

0022-314X/87 $3.00

for the precise statement). The points are the following. The first one is that the condition is stated in the form of the divisibility of special values of L-functions by $\mathfrak{p}$, instead of the independence of Hurwitz numbers modulo $\mathfrak{p}$ in [10]. The second one is that our criterion gives a necessary and sufficient condition, whereas that of Robert in the case where p remains prime in K is a sufficient condition for the divisibility of a relative class number of M by p.

1. Logarithmic Derivatives and Local Units

We retain the notation used in the Introduction. In particular, p is a prime not dividing $6h$ and $\mathfrak{p}$ is a prime ideal of K dividing p. For an integral ideal $\mathfrak{g}$ of K, let $I(\mathfrak{g})$ be the ray class group modulo $\mathfrak{g}$, and $K(\mathfrak{g})$ the maximal ray class field modulo $\mathfrak{g}$. Hence $H = K(\mathfrak{o})$. Let F be a cyclic extension of H of degree $N\mathfrak{p} - 1$, which is totally ramified at all primes lying above p. Later, we take as F the field generated by $\mathfrak{p}$ division points of an elliptic curve E with complex multiplication by K, the definition of which will be given in Section 2. Let $\mathfrak{f}_0$ be as in the Introduction, and L be a subfield of $K(\mathfrak{f}_0)$. Let M be an extension of L contained in LF, which is abelian over K and totally ramified at all primes of L dividing p. We denote the Galois group $\mathrm{Gal}(M/K)$ of the extension M/K by G, and by G_Z (resp. G_T) the decomposition (resp. inertia) subgroup of G for $\mathfrak{p}$. Then $G_T \simeq \mathrm{Gal}(M/L) \simeq \mathrm{Gal}(MH \cap F/H)$. We assume $|G|$, the order of G, is prime to p. Let $\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_s$ be the decomposition into prime ideals in L and let $\bar{\mathfrak{P}}_i$ be the unique prime ideal of M lying above $\mathfrak{P}_i$. Let $m = [M : K]$. Then $\mathfrak{P}_i = \bar{\mathfrak{P}}_i^m$. Let $M_{\mathfrak{P}_i}$ be the completion of M at $\bar{\mathfrak{P}}_i$ and $\mathfrak{O}_{M,\mathfrak{P}_i}$ be the ring of $\bar{\mathfrak{P}}_i$-adic integers in $M_{\mathfrak{P}_i}$. For each positive integer n, put

$$U_{M,i}^{(n)} = \{u \in \mathfrak{O}_{M,\mathfrak{P}_i}^{\times} \mid u \equiv 1 \bmod \bar{\mathfrak{P}}_i^n\},$$

and let $U_M^{(n)}$ be the direct product of $U_{M,i}^{(n)}$. Let Π_i be a prime element of $\mathfrak{O}_{M,\mathfrak{P}_i}$ and $\{w_j,\ 1 \leqslant j \leqslant t\}$ be a $\mathbf{Z}_p$-basis of $\mathfrak{O}_{L,\mathfrak{P}_i}$, where $t = [L_{\mathfrak{P}_i} : \mathbf{Q}_p]$. If p ramifies in K, we take w_j so that half of them are included in $\mathfrak{P}_i$. Put

$$V_i(n) = \prod_{j=1}^{t} (1 + \Pi_i^n w_j)^{\mathbf{Z}_p}.$$

Then we can prove easily

Lemma 1.1.

$$(1) \qquad U_{M,i}^{(1)} = \prod_{1 \leqslant n \leqslant m-1} V_i(n)\, U_{M,i}^{(m)}.$$

$$(2) \qquad U_{M,i}^{(1)p} U_{M,i}^{(m)} = \prod_{1 \leqslant pn \leqslant m-1} V_i(pn)\, U_{M,i}^{(m)}.$$

We define a set of integers $\mathscr{K}$ by

$$\mathscr{K} = \{k = qn \mid (k, p) = 1,\ 1 \leqslant n \leqslant m-1\},$$

where $q = (N\mathfrak{p}-1)/m$. When $\mathfrak{p} = (p)$, let $k(p)$ be the positive integer which satisfies $k(p) \equiv pk \bmod (N\mathfrak{p}-1)$ and $1 \leqslant k(p) \leqslant N\mathfrak{p}-1$. Let $\mathscr{K}_2$ be the subset consisting of $k \in \mathscr{K}$ such that $k(p) = pk$, and let $\mathscr{K}_1$ be the complement of $\mathscr{K}_2$ in $\mathscr{K}$.

In the rest of this section, we assume L contains H. Let L' be an unramified extension of $L_{\mathfrak{P}_i}$, and Λ a prime element of the completion F_i of F at the prime lying above $\mathfrak{p}_i = \mathfrak{P}_i \cap H$ such that $\Lambda^{N\mathfrak{p}-1}$ is contained in $H_{\mathfrak{p}_i}$. Then a unit u of $L'F_i$, which is congruent to 1 modulo (Λ), can be expanded as

$$u = 1 + \sum_{n=1}^{\infty} a_n \Lambda^n, \qquad a_n \in \mathfrak{O}_{L'},$$

where $\mathfrak{O}_{L'}$ is the ring of $\mathfrak{P}_i$-adic integers in L'. Put $f_u(T) = 1 + \sum_{n=1}^{\infty} a_n T^n$ and

$$T\frac{d \log f_u(T)}{dT} = \sum_{k=1}^{\infty} \alpha_k T^k.$$

Then for each k, $1 \leqslant k \leqslant N\mathfrak{p}-1$, the kth logarithmic derivative of u with respect to Λ is defined by

$$\varphi_{k,\Lambda}(u) \equiv \alpha_k \qquad \bmod \mathfrak{P}_i.$$

We extend $\varphi_{k,\Lambda}$ to $(L'F_i)^\times$ by putting $\varphi_{k,\Lambda}(\Lambda) \equiv 0$ and $\varphi_{k,\Lambda}(\zeta) \equiv 0$ if the order of ζ is finite and prime to p. Let $\mathfrak{O}_L$ be the ring of integers in L. Then $\varphi_{k,\Lambda}$ gives rise to a homomorphism

$$\varphi_{k,\Lambda} : U_{M,i}^{(1)} \to \mathfrak{O}_L/\mathfrak{P}_i.$$

For $u \in U_{M,i}^{(1)}$, put

$$\varphi_i(u) = (\varphi_{k,\Lambda}(u))_{k \in \mathscr{K}} \in \bigoplus_{k \in \mathscr{K}} \mathfrak{O}_L/\mathfrak{P}_i.$$

Then we have

PROPOSITION 1.2. *φ_i induces an isomorphism*

$$\varphi_i : U_{M,i}^{(1)}/U_{M,i}^{(m)}U_{M,i}^{(1)p} \xrightarrow{\sim} \bigoplus_{k \in \mathscr{K}} \mathfrak{O}_L/\mathfrak{P}_i.$$

Proof. It is easy to see $U_{M,i}^{(m)}U_{M,i}^{(1)^p}$ is contained in the kernel of φ_i. We may assume $\Pi_i = a\Lambda^q$ for $a \in O_L^\times \cdot \mathfrak{P}_i$. Put $u_n = 1 + \alpha\Pi_i^n$ for $\alpha \in \mathfrak{O}_{L,\mathfrak{P}_i}$ and a positive integer n. Then

$$\varphi_{k,\Lambda}(u_n) \equiv \begin{cases} 0 & \text{if } k < nq, \\ \alpha nqa^n & \text{if } k = nq. \end{cases}$$

The surjectivity follows from this. Comparing the dimension of both spaces over $\mathbf{F}_p$, we can conclude φ_i is an isomorphism by Lemma 1.1.

Put $W_i = U_{M,i}^{(1)}/U_{M,i}^{(m)}U_{M,i}^{(1)^p}$. Then W_i is a $\mathbf{F}_p[G_Z]$-module and by φ_i, $\oplus_{k\in\mathscr{K}} \mathfrak{O}_L/\mathfrak{P}_i$ can be seen as a $\mathbf{F}_p\ [G_Z]$-module. The action of G_Z on $\oplus_{k\in\mathscr{K}} \mathfrak{O}_L/\mathfrak{P}_i$ can be described as follows. Extend $g \in G_Z$ to an automorphism $\tilde{g}$ of the Galois closure of $L_{\mathfrak{P}_i}F_i$ over $K_\mathfrak{p}$, and put $c_k(g) \equiv (\Lambda^{\tilde{g}}/\Lambda)^k$. Then $c_k(g)$ depends only on g, and the action of g on the k-component is given by

$$a^{\langle g\rangle} \equiv c_k(g)\, a^g.$$

On G_T, c_k is a character. Put $W = \oplus_i W_i$ (considered additively). Let $\bar{X}_M$ be the group of all characters of G with values in $\bar{\mathbf{F}}_p$ and for $\bar{\chi} \in X_M$, let $W(\bar{\chi}) = (W \otimes_{\mathbf{F}_p} \bar{\mathbf{F}}_p)(\bar{\chi})$ be the $\bar{\chi}$-component of $W \otimes_{\mathbf{F}_p} \bar{\mathbf{F}}_p$. We denote by 1_χ the idempotent of $\bar{\mathbf{F}}_p[G]$ for $\bar{\chi}$. In the following, we study the structure of $W(\bar{\chi})$. Let pr_i be the projection of W onto W_i . Then we see

$$\mathrm{pr}_i\colon W(\bar{\chi}) \xrightarrow{\sim} W_i(\bar{\chi}|_{G_Z}). \tag{1.1}$$

First we treat the case where p decomposes or ramifies in K. In this case, we have

$$W_i \otimes_{\mathbf{F}_p} \bar{\mathbf{F}}_p \simeq \mathrm{Ind}_{G_T}^{G_Z}(\mathrm{Ind}_{\{1\}}^{G_T}(1) - 1), \tag{1.2}$$

where 1 denotes the trivial representation. If the tamely ramified extension $M_{\mathfrak{P}_i}/K_\mathfrak{p}$ splits (cf. [6, 2.1]), this follows from Lemma 1 in [6]. If it does not split, there exists an unramified extension L' of $L_{\mathfrak{P}_i}$ such that $L'M_{\mathfrak{P}_i}/K_\mathfrak{p}$ splits and $[L'\colon L_{\mathfrak{P}_i}]$ is prime to p. The general case can be reduced to the splitting case by considering $\mathrm{Gal}(L'M_{\mathfrak{P}_i}/M_{\mathfrak{P}_i})$ invariant subspaces. Let S_k be the k-component of $\oplus_{k\in\mathscr{K}} \mathfrak{O}_L/\mathfrak{P}_i$. Then by (1.2), we see

$$S_k \otimes_{\mathbf{F}_p} \bar{\mathbf{F}}_p \simeq \mathrm{Ind}_{G_T}^{G_Z}(c_k|_{G_T}), \tag{1.3}$$

as $\bar{\mathbf{F}}_p[G_Z]$-modules. We fix an embedding of $\mathfrak{O}_L/\mathfrak{P}_i$ into $\bar{\mathbf{F}}_p$ and consider $\mathfrak{O}_L/\mathfrak{P}_i$ as a subset of $\bar{\mathbf{F}}_p$. This inclusion induces a map

$$\lambda\colon S_k(\bar{\chi}|_{G_Z}) \to \bar{\mathbf{F}}_p.$$

LEMMA 1.4. *If* $\bar{\chi}|_{G_T} = c_k|_{G_T}$ *for* $k \in \mathscr{K}$, λ *induces an isomorphism*

$$\lambda : S_k(\bar{\chi}|_{G_Z}) \xrightarrow{\sim} \bar{\mathbf{F}}_p.$$

Proof. Since $\dim_{\bar{\mathbf{F}}_p} S_k(\bar{\chi}|_{G_Z}) = 1$ by (1.3), it is enough to show that λ is not trivial. We have an isomorphism

$$S_k \otimes_{\mathbf{F}_p} \bar{\mathbf{F}}_p \simeq \bigoplus_{g \in G_Z/G_T} \bar{\mathbf{F}}_p$$

by the map $a \otimes b \mapsto (a^g b)_{g \in G_Z/G_T}$. Let e be the idempotent of $\bar{\mathbf{F}}_p[G_Z]$ for $\bar{\chi}|_{G_Z}$. Then the g-component of the image of $e(a \otimes 1)$ is

$$|G_Z|^{-1} \sum_{h \in G_Z} (c_k(h)\, a^h)^g\, \bar{\chi}(h)^{-1} = c_k(g)^{-1}\, \bar{\chi}(g) |G_Z|^{-1} \sum_{h \in G_Z} c_k(h)\, a^h \bar{\chi}(h)^{-1}.$$

Here we used the relation $c_k(hh') = c_k(h)^{h'} c_k(h')$. Our assertion follows from this.

By (1.1) and Lemma 1.4, we obtain

PROPOSITION 1.5. *Assume* p *decomposes or ramifies in* K *and* $\bar{\chi} \in X_M$ *satisfies* $\bar{\chi}|_{G_T} = c_k|_{G_T}$ *for* $k \in \mathscr{K}$. *For* $u \otimes x \in W \otimes_{\mathbf{F}_p} \bar{\mathbf{F}}_p$, put

$$\Phi_k(1_{\bar{\chi}}(u \otimes x)) = |G|^{-1} \sum_{g \in G} \varphi_{k,A}(pr_i(u^g))\, x \bar{\chi}(g)^{-1}.$$

Then Φ_k *induces an isomorphism*

$$\Phi_{\bar{\chi}} : W(\bar{\chi}) \xrightarrow{\sim} \bar{\mathbf{F}}_p.$$

Now we assume p remains prime in K. Let $S_k = \mathfrak{O}_L/\mathfrak{P}_i$ with the action of G_Z defined by

$$a^{\langle g \rangle} \equiv c_k(g)\, a^g \qquad \mathrm{mod}\ \mathfrak{P}_i.$$

Since (p) decomposes completely in H, c_k is a character of G_Z, and the action of G_Z is $\mathbf{F}_{p^2}$-linear. We see easily

$$S_k \otimes_{\mathbf{F}_{p^2}} \bar{\mathbf{F}}_p \simeq \mathrm{Ind}_{G_T}^{G_Z}(c_k|_{G_T}),$$

and

$$S_k \otimes_{\mathbf{F}_p} \bar{\mathbf{F}}_p \simeq S_k \otimes_{\mathbf{F}_{p^2}} \bar{\mathbf{F}}_p \oplus S_{k(p)} \otimes_{\mathbf{F}_{p^2}} \bar{\mathbf{F}}_p,$$

by the map $a \otimes b \mapsto (a \otimes b, a^p \otimes b)$, since $c_k(g)^p \equiv c_{k(p)}(g)$. In the same way as above, we obtain

PROPOSITION 1.6. *Assume p remains prime in K. Let $\bar{\chi}|_{G_T} = c_k|_{G_T}$.* For $u \otimes x \in W \otimes_{\mathbf{F}_p} \bar{\mathbf{F}}_p$, put

$$\Phi_k(1_{\bar{\chi}}(u \otimes x)) = |G|^{-1} \sum_{g \in G} \varphi_{k,\Lambda}(pr_i(u^g))\, x\bar{\chi}(g)^{-1},$$

$$\Phi'_k(1_{\bar{\chi}}(u \otimes x)) = |G|^{-1} \sum_{g \in G} \varphi_{k(p),\Lambda}(pr_i(u^g))^p\, x\bar{\chi}(g)^{-1}.$$

(1) *If $k \in \mathscr{K}_1$, one has an isomorphism*

$$\Phi_{\bar{\chi}} : W(\bar{\chi}) \xrightarrow{\sim} \bar{\mathbf{F}}_p \oplus \bar{\mathbf{F}}_p,$$

defined by $\Phi_{\bar{\chi}}(1_{\bar{\chi}}(u \otimes x)) = (\Phi_k(1_{\bar{\chi}}(u \otimes x)), \Phi'_k(1_{\bar{\chi}}(u \otimes x)))$.

(2) *If $k \in \mathscr{K}_2$ (resp. $k(p) \in \mathscr{K}_2$), one has an isomorphism*

$$\Phi_{\bar{\chi}} : W(\bar{\chi}) \xrightarrow{\sim} \bar{\mathbf{F}}_p,$$

defined by $\Phi_{\bar{\chi}}(1_{\bar{\chi}}(u \otimes x)) = \Phi_k(1_{\bar{\chi}}(u \otimes x))$ (resp. $\Phi'_k(1_{\bar{\chi}}(u \otimes x))$).

We note $\Phi_k(1_{\bar{\chi}}(u \otimes x)) = 0$, $\Phi'_k(1_{\bar{\chi}}(u \otimes x)) = 0$ if the condition $\bar{\chi}|_{G_T} = c_k|_{G_T}$ is not satisfied.

PROPOSITION 1.7. *Let $\bar{\chi}|_{G_T} = c_k|_{G_T}$. If $k \in \mathscr{K}_2$ or $k(p) \in \mathscr{K}_2$, one has*

$$\Phi_k(x) \equiv 0 \bmod \mathfrak{P}_i \Leftrightarrow \Phi'_k(x) \equiv 0 \bmod \mathfrak{P}_i,$$

for $x \in W(\bar{\chi})$.

Proof. We give a proof only for the case $k \in \mathscr{K}_2$. The case $k(p) \in \mathscr{K}_2$ can be treated in the same way. Let $k = nq$ and let $u_n = 1 + \alpha \Pi_i^n$ be as in the proof of Proposition 1.2. Then we see

$$\varphi_{k(p),\Lambda}(u_n) \equiv \varphi_{k,\Lambda}(u_n)^p \qquad \bmod \mathfrak{P}_i.$$

Let $\tilde{u}_n$ be the element of $U_M^{(1)}$ such that the i-component is u_n and the other components are 1. Then we see

$$\Phi'_k(1_{\bar{\chi}}(\tilde{u}_n \otimes 1)) \equiv (\Phi_k(1_{\bar{\chi}}(\tilde{u}_n \otimes 1)))^{p^2} \qquad \bmod \mathfrak{P}_i.$$

It is easy to see that we can choose α so that $\Phi_k(1_{\bar{\chi}}(\tilde{u}_n \otimes 1)) \not\equiv 0 \bmod \mathfrak{P}_i$. This proves our assertion.

2. Logarithmic Derivatives of Elliptic Units

We review the results on elliptic units by Siegel, Ramachandra and Robert with some comments (cf. [12, 8–10]). Let $\mathfrak{g}$ be an integral ideal of K different from $\mathfrak{o}$. For an ideal $\mathfrak{a}$ prime to $\mathfrak{g}$, let $C_{\mathfrak{a}}$ denote the class in $I(\mathfrak{g})$ containing $\mathfrak{a}$ and $(\mathfrak{a}, K(\mathfrak{g})/K)$ the Artin symbol of $\mathfrak{a}$ on $K(\mathfrak{g})$. Let $A(\mathfrak{g})$ be the set of couples $(\tau, \mathscr{L})$ consisting of a lattice $\mathscr{L}$ in $\mathbf{C}$ such that $\{\lambda \in \mathbf{C} \mid \lambda\mathscr{L} \subset \mathscr{L}\} = \mathfrak{o}$ and $\tau \in \mathbf{C}$ such that $\tau^{-1}\mathscr{L} \cap \mathfrak{o} = \mathfrak{g}$. We say $(\tau, \mathscr{L})$ and $(\tau', \mathscr{L}')$ are equivalent if there exists $\alpha \in K$ such that $\mathscr{L}' = \alpha\mathscr{L}$ and $\tau' - \alpha\tau \in \mathscr{L}'$. Then the application $(\tau, \mathscr{L}) \to (\tau^{-1}\mathscr{L})^{-1}\mathfrak{g}$ induces a bijection between $A(\mathfrak{g})/\sim$ and $I(\mathfrak{g})$. We denote the image of $(\tau, \mathscr{L})$ in $I(\mathfrak{g})$ by $C(\tau, \mathscr{L})$.

Let $\mathfrak{H} = \{z \in \mathbf{C} \mid \mathrm{Im}(z) > 0\}$. For $w \in \mathbf{C}$ and $z \in \mathfrak{H}$, let

$$\theta_1(w, z) = \sum_{n=-\infty}^{\infty} \exp(\pi i(n + 1/2)^2 z + 2\pi i(n + 1/2)(w - 1/2)),$$

and $\eta(z)$ the Dedekind η-function. For $C = C(\tau, \mathscr{L})$, let $\{\omega_1, \omega_2\}$ be a basis of $\mathscr{L}$ such that $\mathrm{Im}(\omega_2/\omega_1) > 0$. Define

$$\varphi_{\mathfrak{g}}(C) = (\exp(\pi i(z - \bar{z})^{-1}((\tau/\omega_1)^2 - (\tau/\omega_1)(\overline{\tau/\omega_1}))) \eta(z)^{-1} \theta_1(\tau/\omega_1, z))^{12g},$$

where $z = \omega_2/\omega_1$ and g is the positive integer such that $\mathfrak{g} \cap \mathbf{Z} = g\mathbf{Z}$.

Theorem 2.1 (Siegel and Ramachandra). (1) *For C, $C' \in I(\mathfrak{g})$, $\varphi_{\mathfrak{g}}(C)$ is contained in $K(\mathfrak{g})$, and $\varphi_{\mathfrak{g}}(C)/\varphi_{\mathfrak{g}}(C')$ is a unit. Let $\mathfrak{a}$ be an integral ideal prime to $\mathfrak{g}$. Then*

$$\varphi_{\mathfrak{g}}(C)^{(\mathfrak{a}, K(\mathfrak{g})/K)} = \varphi_{\mathfrak{g}}(CC_{\mathfrak{a}}).$$

(2) *Let χ be a character of $I(\mathfrak{g})$ with values in $\mathbf{C}$ such that the conductor $\mathfrak{f}(\chi) = \mathfrak{g}$, and $L(s, \chi)$ the L-function of K with χ. Then one has*

$$L'(0, \chi) = -(6w(\mathfrak{g})\, g)^{-1} \sum_{C \in I(\mathfrak{g})/\mathrm{Ker}\,\chi} \chi(C) \log |N_{K(\mathfrak{g})/M_\chi}(\varphi_{\mathfrak{g}}(C))|,$$

where $w(\mathfrak{g})$ is the number of units of K congruent to 1 modulo $\mathfrak{g}$, and M_χ is the subfield of $K(\mathfrak{g})$ corresponding to Ker χ.

For $w \in \mathbf{C}$ and $z = \omega_2/\omega_1$, put

$$\theta(w, \mathscr{L}) = (\exp(\pi i(z - \bar{z})^{-1}(w/\omega_1)) \eta(z)^{-1} \theta_1(w/\omega_1, z))^{12},$$

and for an integral ideal $\mathfrak{a}$ prime to $\mathfrak{g}$, put

$$\theta(w, \mathscr{L}; \mathfrak{a}) = \theta(w, \mathscr{L})^{N\mathfrak{a}}/\theta(w, \mathfrak{a}^{-1}\mathscr{L}).$$

Then $\theta(\tau, \mathscr{L}; \mathfrak{a})$ depends only on $C(\tau, \mathscr{L})$. We denote it by $\theta(C, \mathfrak{a})$.

THEOREM 2.2 (Robert). *Let* $\mathfrak{a}$, $\mathfrak{b}$ *be integral ideals of* K *prime to* $\mathfrak{g}$. *Then*:

(1) $\theta(C, \mathfrak{a})$ *is contained in* $K(\mathfrak{g})$.

(2) $\theta(C, \mathfrak{a})^{(\mathfrak{b}, K(\mathfrak{g})/K)} = \theta(CC_{\mathfrak{b}}, \mathfrak{a})$.

(3) $\varphi_{\mathfrak{g}}(C)^{N\mathfrak{a}}/\varphi_{\mathfrak{g}}(CC_{\mathfrak{a}}) = \theta(C, \mathfrak{a})^{g}$.

Let $\mathfrak{f}_0$ be as in Section 1, and let $\mathfrak{f} = \mathfrak{p}\mathfrak{f}_0$. Let E be an elliptic curve defined over H such that $\theta: \mathfrak{o} \simeq \mathrm{End}(E)$. We fix θ so that the action of $\mathfrak{o}$ on the differential form of the first kind is the identity. We assume E has good reduction at each prime dividing $\mathfrak{f}$. Let $\mathbf{p}$ be a prime ideal of H lying above $\mathfrak{p}$, and let

$$y^2 = 4x^3 - g_2 x - g_3$$

be a Weierstrass model of E which has good reduction at $\mathbf{p}$. We assume the period lattice $\mathscr{L}$ of E by $y^{-1}dx$ is of the form $\mathfrak{f}\Omega_\infty$. There exists an elliptic curve satisfying the above conditions. Let $F = H(E_{\mathfrak{p}})$.

Let $\wp(w) = \wp(w, \mathscr{L})$ be the Weierstrass $\wp$ function attached to $\mathscr{L}$, and put $\xi(w) = (\wp(w), \wp'(w))$. Let $t = -2x/y$. Then there exists a formal power series $a(t)$ such that $x = t^{-2}a(t)$ and $y = -2t^{-3}a(t)$. The coefficients of $a(t)$ are contained in $\mathfrak{O}_{H,\mathbf{p}}$ and its constant term is 1. Let $\hat{E}$ be the formal group giving the kernel $E_{1,\mathbf{p}}$ of the reduction modulo $\mathbf{p}$ on E. Then the application $t \mapsto (t^{-2}a(t), \ -2t^{-3}a(t))$ gives an isomorphism between $\hat{E}(\bar{m})$ and $E_{1,\mathbf{p}}(\bar{H}_{\mathbf{p}})$, where $\bar{m}$ is the maximal ideal of an algebraic closure $\bar{H}_{\mathbf{p}}$ of $H_{\mathbf{p}}$. For $\hat{E}$, there exists a formal group $\mathscr{E}$ such that $\psi: \hat{E} \simeq \mathscr{E}$ and the action of $(N\mathfrak{p} - 1)$th roots of unity ζ in $\mathfrak{o}_{\mathfrak{p}}$ is given by

$$[\zeta]\, u = \zeta u,$$

where $u = \psi(t)$.

Let $\tau = \Omega_\infty$ and $\mathscr{L} = \mathfrak{f}\Omega_\infty$. Then $(\tau, \mathscr{L}) \in A(\mathfrak{f})$ and $C(\tau, \mathscr{L})$ is the unit class C_0 in $I(\mathfrak{f})$. We can prove easily

LEMMA 2.3. *There exist* τ_1, τ_2 *such that* $\tau = \tau_1 + \tau_2$, $\tau_1^{-1}\mathscr{L} \cap \mathfrak{o} = \mathfrak{p}$ *and* $\tau_2^{-1}\mathscr{L} \cap \mathfrak{o} = \mathfrak{f}_0$. *They can be chosen so that* $\tau_2^{-1}\mathscr{L} = \mathfrak{f}_0\mathfrak{c}^{-1}$ *with an integral ideal* $\mathfrak{c}$ *prime to* $\mathfrak{f}$, *and the class* τ_1 *modulo* $\mathscr{L}$ *is well defined.*

Put $Q = \xi(\tau_1)$. Then Q is a primitive $\mathfrak{p}$ division point on E and $\Lambda = \psi(t(Q))$ satisfies the condition for Λ in Section 1 (cf. [9, Sect. 5]).

Let $\mathfrak{f}_0'$ be a divisor of $\mathfrak{f}_0$, and let $\mathfrak{f}' = \mathfrak{p}\mathfrak{f}_0'$. Let E' be the quotient of E by the subgroup of $\mathfrak{f}_0/\mathfrak{f}_0'$ division points, and $y^2 = 4x^3 - g_2' x - g_3'$ a Weierstrass model of E' which has good reduction at $\mathbf{p}$. We may assume the period lattice $\mathscr{L}'$ of E' for $y^{-1}dx$ is $\mathfrak{f}'\Omega_\infty$. We note $(\tau, \mathscr{L}') \in A(\mathfrak{f}')$, $C(\tau, \mathscr{L}')$ is the unit class C_0' in $I(\mathfrak{f}')$, and τ_1 and τ_2 satisfy the condition in Lemma 2.3 for

$\mathscr{L}'$ and $\mathfrak{f}_0'$ with the same $\mathfrak{c}$. Let λ be the natural map of E onto E'. Then $\lambda(Q) = (\tau_1 \bmod \mathscr{L}')$ and λ induces an isomorphism of $\hat{E}$ onto $\hat{E}'$ over $\mathfrak{O}_{H,\mathfrak{p}}$. Hence we may take the same $\mathscr{E}$ and Λ for $\hat{E}$ and $\hat{E}'$.

LEMMA 2.4. *Let $\alpha \in K^\times$ be prime to $\mathfrak{f}$. Then*

$$c_k(((\alpha), K(\mathfrak{f})/K)) \equiv \alpha^k \bmod \mathfrak{p}.$$

Proof. Let $\tilde{\alpha}$ be the element of the idele group $K_A^\times$ of K such that the components at primes dividing $\mathfrak{f}$ are α^{-1} and the other components are 1. For $\beta \in K_A^\times$, let $[\beta, K]$ be the image of β in $\mathrm{Gal}(K_{ab}/K)$ through the Artin map. Then the action on M of $((\alpha), K(\mathfrak{f})/K)$ coincides with that of $[\tilde{\alpha}, K]$. Let x be an element of the maximal compact subgroup of $H_A^\times$ such that $N_{H/K}(x) = \tilde{\alpha}$. We may assume the components at primes not dividing $\mathfrak{f}$ are 1. Since E has good reduction at primes dividing $\mathfrak{f}$, by Proposition 7.40 and the proof of Theorem 7.42 of [11], we have

$$Q^{[x,H]} = \theta(\alpha)\, Q.$$

Our assertion follows from this.

For a positive integer k and $w \in \mathbf{C}$, put

$$H_k(w, s, \mathscr{L}') = \sum{}' \frac{(\bar{w} + \bar{\omega})^k}{|w + \omega|^{2s}}, \qquad \mathrm{Re}(s) > 1 + k/2,$$

where the sum is taken over all $\omega \in \mathscr{L}' = \mathfrak{f}'\Omega_\infty$ except $-w$ if $w \in \mathscr{L}'$. Then as a function of s, H_k can be continued to the whole s-plane meromorphically. For $\tau \in Q\mathscr{L}'$, put

$$E_k(\tau, \mathscr{L}') = H_k(\tau, k, \mathscr{L}').$$

Then if $\mathfrak{g}\tau \subset \mathscr{L}'$ for an integral ideal $\mathfrak{g}$, $E_k(\tau, \mathscr{L}')$ is contained in $H(E_\mathfrak{g}')$, and it holds for $\tau \notin \mathscr{L}'$

$$w\frac{d}{dw}\log\theta(w + \tau, \mathscr{L}'; \mathfrak{a}) = 12(-1)^{k-1} \sum_{k \geq 1} (N\mathfrak{a}E_k(\tau, \mathscr{L}') - E_k(\tau, \mathfrak{a}^{-1}\mathscr{L}'))\, w^k, \tag{2.1}$$

where $\mathfrak{a}$ is an integral ideal prime to $\mathfrak{f}'$(cf. [3, (2.1) Theorem (i)]).

Let $\bar{\mathbf{Q}}$ be the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$ and $\mathbf{C}_p$ the completion of the algebraic closure of $\mathbf{Q}_p$. We denote the maximal ideal of the valuation ring of $\mathbf{C}_p$ by P. We fix an embedding of $\bar{\mathbf{Q}}$ into $\mathbf{C}_p$ so that $P \cap H = \mathfrak{p}$.

PROPOSITION 2.5. *For an integer k, $1 \leqslant k \leqslant N\mathfrak{p} - 2$, one has*

$$\varphi_{k,\Lambda}(\theta(C'_0, \mathfrak{a})) \equiv 12(-1)^{k-1}\,(N\mathfrak{a}E_k(\tau_2, \mathscr{L}') - E_k(\tau_2, \mathfrak{a}^{-1}\mathscr{L}')) \qquad \mathrm{mod}\ P.$$

This can be proved in the same way as [9, Proposition 46] and [5, Sect. 5, Proposition] by(2.1).

COROLLARY 2.6. *Let $\mathfrak{b}$ be an integral ideal of K prime to $\mathfrak{f}'$. Then*

$$\varphi_{k,\Lambda}(\theta(C'_0, \mathfrak{a})^{(\mathfrak{b}, K(\mathfrak{f}')/K)}) \equiv 12(-1)^{k-1}\,(N\mathfrak{a}E_k(\tau_2, \mathfrak{b}^{-1}\mathscr{L}') - E_k(\tau_2, (\mathfrak{ab})^{-1}\mathscr{L}')) \qquad \mathrm{mod}\ P.$$

This follows from

$$\theta(C'_0, \mathfrak{a})^{(\mathfrak{b}, K(\mathfrak{f}')/K)} = \theta(C'_0, \mathfrak{b})^{N\mathfrak{a}}/\theta(C'_0, \mathfrak{ab}).$$

LEMMA 2.7. *Let $\mathfrak{a}$ and $\mathfrak{a}'$ be integral ideals of K prime to $\mathfrak{f}'$. Assume there exists α such that $\mathfrak{a}' = \alpha\mathfrak{a}$ and $\alpha \equiv 1 \bmod \mathfrak{f}'_0$. Then*

$$E_k(\tau_2, \mathfrak{a}'^{-1}\mathscr{L}') = \alpha^k E_k(\tau_2, \mathfrak{a}^{-1}\mathscr{L}').$$

Proof. Since $E_k(\tau_2, \mathfrak{a}'^{-1}\mathscr{L}') = \alpha^k E_k(\alpha\tau_2, \mathfrak{a}^{-1}\mathscr{L}')$, it is enough to show $\alpha\tau_2 - \tau_2 \in \mathfrak{a}^{-1}\mathscr{L}'$. This can be verified easily.

COROLLARY 2.8. *Let $\tilde{\omega}$ be an element of K such that $\tilde{\omega} \in \mathfrak{p}$ and $\tilde{\omega} \notin \mathfrak{p}^2$. Let $l = 1$, 2, or $p+1$ according to whether p decomposes, ramifies, or remains prime in K. Then $E_k(\tau_2, \mathfrak{a}^{-1}\mathscr{L}')$ is P-integral if $k \neq l$ or if p decomposes in K and $\bar{\mathfrak{p}}$ does not divide $\mathfrak{f}'_0$, where $\bar{\mathfrak{p}}$ denotes the conjugate of $\mathfrak{p}$. Otherwise, $\tilde{\omega}E_k(\tau_2, \mathfrak{a}^{-1}\mathscr{L}')$ is a P-unit.*

Proof. Let $\tau_2^{-1}\mathscr{L} = f\mathfrak{c}^{-1}$ with $\mathfrak{c}$ prime to $\mathfrak{f}$ and let

$$\zeta = \exp(24Nc\pi i/p) = \theta(C'_0, (\alpha))/\theta(C'_0, (\bar{\alpha})),$$

where $\alpha = 1 + N(\mathfrak{f}'/p)\,p\sqrt{D}$ if p decomposes and $\bar{\mathfrak{p}} \mid \mathfrak{f}'_0$ or p remains prime, and $\alpha = 1 + N(\mathfrak{f}'/\mathfrak{p})\sqrt{D}$ if p ramifies. Here D is the discriminant of K. By Lemma 2.7, we have

$$\varphi_{l,\Lambda}(\zeta) \equiv 12(-1)^{l-1}\,(\bar{\alpha}^l - \alpha^l)\,E_l(\tau_2, \mathscr{L}') \qquad \mathrm{mod}\ P. \tag{2.2}$$

Our assertion can be deduced from this in the same way as [10, Proposition 16].

3. Elliptic Units and Class Number Formulas

Let M and L be as in Section 1, and N be a subfield of M containing L. Let X_M be the group of all characters of G with values in $\bar{\mathbf{Q}}$, and let $X_{M/N}$ be its subset consisting of χ such that $\mathrm{Ker}\,\chi \not\supset \mathrm{Gal}(M/N)$. We consider $\chi \in X_M$ also to be a character of $I(\mathfrak{f})$ or $I(\mathfrak{f}(\chi))$ through the Artin map. For an algebraic number field S, we denote by h_S, R_S, and $w(S)$ the class number, the regulator, and the number of roots of unity of S, respectively. Then we have

$$h_{M/N} = h_M/h_N = \frac{R_N w(M)}{R_M w(M)} \prod_{\chi \in X_{M/N}} \mathscr{L}'(0, \chi). \tag{3.1}$$

By the embedding of $\bar{\mathbf{Q}}$ into $\mathbf{C}_p$ fixed in Section 2, we consider χ also as a character with values in $\mathbf{C}_p$. Let ω be the Teichmüller character modulo p, and put $\omega_K = \omega \circ N_{K/Q}$. For $\chi \in X_M$, let r_χ be the order of χ. We say χ and χ' are equivalent if they generate the same subgroup of X_M, and denote the equivalence class containing χ by $\hat{\chi}$.

LEMMA 3.1. *For $\chi \in X_M$, $\chi \neq 1$, and an integral ideal $\mathfrak{a}$ of K, put*

$$A_{\hat{\chi}}(\mathfrak{a}) = \prod_{\rho \in \hat{\chi}} (N\mathfrak{a} - \rho((\mathfrak{a}, K(\mathfrak{f}(\chi))/K))).$$

Then there exists an integral ideal $\mathfrak{a}_\chi$ prime to $\mathfrak{f}(\chi)$ such that $A_{\hat{\chi}}(\mathfrak{a}_\chi)$ is prime to p if $\hat{\chi} \neq \hat{\omega}_K$, and is divided by p exactly once if $\hat{\chi} = \hat{\omega}_K$. For $\hat{\chi} = \hat{\omega}_K$, we may take $\mathfrak{a}_\chi = (\alpha_\chi)$ with $\alpha_\chi = 1 + N(\mathfrak{f}(\chi)/p)\,p$ if p decomposes or remains prime and with $\alpha_\chi = 1 + N(\mathfrak{f}(\chi)/\mathfrak{p})\sqrt{D}$ if p ramifies.

Proof. If $\mathrm{Ker}\,\chi \neq \mathrm{Ker}\,\omega_K$, it is easy to see there exists such $\mathfrak{a}_\chi$. If the kernels coincide, $\hat{\chi} = \hat{\omega}_K$. For $\chi = \omega_K$, $A_{\hat{\chi}}(\mathfrak{a}) = \Phi_{p-1}(N\mathfrak{a})$ with the $(p-1)$th cyclotomic polynomial Φ_{p-1}. It is easily checked that $(N\alpha_\chi)^{p-1} - 1$ is divided by p exactly once for α_χ in our lemma. This completes the proof.

For $\chi \in X_M$, let $G_\chi = \mathrm{Ker}\,\chi$, and let M_χ be the subfield of M corresponding to G_χ. Let $d_{\hat{\chi}}$ be the discriminant of the field of r_χth roots of unity. Let $r = |G|$, and put

$$Q_M = \sqrt{r^{r-2} \Big/ \left(\prod_{\hat{\chi}} d_{\hat{\chi}} \right)}.$$

Define Q_N for $\mathrm{Gal}(N/K)$ in the same way. Choose $g_\chi \in G_\chi$ which generates G/G_χ, and put

$$D_{\hat{\chi}} = \prod_{q \mid r_\chi} (1 - g_\chi^{r_\chi/q}),$$

where the product is taken over all primes q dividing r_χ. We define an elliptic unit $\theta_{\hat{\chi}}$ by

$$\theta_{\hat{\chi}} = N_{K(\mathfrak{f}(\chi))/M_\chi}(\theta(C_0', \mathfrak{a}_\chi))^{D_{\hat{\chi}}},$$

and put

$$\Theta_{M/N} = \prod_{\hat{\chi} \in X_{M/N}/\sim} \theta_{\hat{\chi}}^{\mathbf{Z}[G]}.$$

Let E_M be the group of units in M and μ_M the group of roots of unity in M. Let $E_{M/N} = \{\varepsilon \in E_M \mid N_{M/N}(\varepsilon) = 1\}$, and $\mu_{M/N} = \{\eta \in \mu_M \mid N_{M/N}(\eta) = 1\}$. Then $\Theta_{M/N}$ is contained in $E_{M/N}$.

THEOREM 3.2. *Let the notation be as above. Then one has*

$$h_{M/N} = AB[E_{M/N} : \Theta_{M/N}\mu_{M/N}],$$

where

$$A = 2^{-[M:K]+[N:K]} Q_N Q_M^{-1} [E_M : E_{M/N} E_N \mu_M] \prod_{\chi \in X_{M/N}} (6w(\mathfrak{f}(\chi)))^{-1},$$

$$B = w(N)\, w(M)^{-1} \prod_{\hat{\chi} \in X_{M/N}/\sim} A_{\hat{\chi}}(\mathfrak{a}_\chi).$$

Proof. To transform the right-hand side of (3.1), we use the result of Leopoldt [7]. Although he treated the case of cyclotomic units, his result can be applied to our case. By Theorem 2.2, we have

$$A_{\hat{\chi}}(\mathfrak{a}_\chi) \prod_{\rho \in \hat{\chi}} \left(\sum_{g \in G/G_\chi} \rho(g) \log |N_{K(\mathfrak{f}(\chi))/M_\chi}(\varphi_{\mathfrak{f}(\chi)}(C_0'))^g| \right)$$
$$= \prod_{\rho \in \hat{\chi}} \left(f_\rho \sum_{g \in G/G_\chi} \rho(g) \log |N_{K(\mathfrak{f}(\chi))/M_\chi}(\theta(C_0', \mathfrak{a}_\chi))^g| \right).$$

Here $\mathfrak{f}(\rho) \cap \mathbf{Z} = f_\rho \mathbf{Z}$, $f_\rho > 0$. For each $\chi \in X_N$, $\chi \neq 1$, choose a unit e of M_χ such that $\log |e_{\hat{\chi}}| \neq 0$ for $e_{\hat{\chi}} = e^{D_{\hat{\chi}}}$. Put

$$H_N = \prod_{\chi \in X_N - \{1\}} e_{\hat{\chi}}^{\mathbf{Z}[\mathrm{Gal}(N/K)]},$$
$$H_M = \Theta_{M/N} H_N.$$

For a subgroup H of E_M (resp. E_N), let $R_M(H)$ (resp. $R_N(H)$) be the regulator of H defined by $\log |*|$ instead of $\log |*|^2$.

Then by [7, Satz 14, Satz 17, (8), (9) in Sect. 9], we obtain

$$h_{M/N} = AB(R_M(E_M)\, R_N(H_N))^{-1}\, R_N(E_N)\, R_M(H_M).$$

We see

$$\begin{aligned}(R_M(E_M)\, R_N(H_N))^{-1}\, R_N(E_N)\, R_M(H_M) &= [E_M : H_M\mu_M]/[E_N : H_N\mu_N] \\ &= [E_M : E_{M/N}E_N\mu_M][E_{M/N} : \Theta_{M/N}\mu_{M/N}].\end{aligned}$$

This completes the proof.

COROLLARY 3.3. *The p-part of $h_{M/N}$ is equal to the p-part of $[E_{M/N} : \Theta_{M/N}\mu_{M/N}]$.*

Proof. Since $(|G|, p) = 1$, A is prime to p by definition. The p-parts of $w(M)$ and $w(N)$ are different if and only if $\omega_K \in X_{M/N}$. Hence by Lemma 3.1, B is also prime to p.

We note $\mathfrak{f}(\chi)$ is divided by $\mathfrak{p}$ for $\chi \in X_{M/N}$.

PROPOSITION 3.4. *Assume $\chi \in X_{M/N}$ satisfies*

$$\chi(C_{(\alpha)}) \equiv \alpha^k \mod P, \tag{3.2}$$

for α such that $(\alpha, \mathfrak{f}(\chi)) = 1$ and $\alpha \equiv 1 \bmod \mathfrak{f}(\chi)/\mathfrak{p}$. Then there exists a Grössencharacter $\tilde{\chi}$ of K with the properties:

(1) *the conductor $\mathfrak{f}(\tilde{\chi}) = \mathfrak{f}(\chi)/\mathfrak{p}$;*

(2) *$\tilde{\chi}((\alpha)) = \bar{\alpha}^k$ if $\alpha \equiv 1 \bmod \mathfrak{f}(\tilde{\chi})$;*

(3) *$\tilde{\chi}(\mathfrak{a}) \equiv \chi(C_{\mathfrak{a}})^{-1}\, N\mathfrak{a}^k \bmod P$ for $\mathfrak{a}$ prime to $\mathfrak{f}(\chi)$.*

$\tilde{\chi}$ is determined uniquely by the above conditions.

Proof. Let $\chi = \prod_v \chi_v$ considered as a character of $K_A^\times$, and let $\mathfrak{f}_0' = \mathfrak{f}(\chi)/\mathfrak{p}$. Then (3.2) implies $\chi_{\mathfrak{p}}(\alpha) \equiv \alpha^{-k} \bmod P$ for $\alpha \equiv 1 \bmod \mathfrak{f}_0'$. Let α be prime to $\mathfrak{f}(\chi)$ and let β be an element of $K^\times$ such that $\beta \equiv \alpha \bmod \mathfrak{p}$ and $\beta \equiv 1 \bmod \mathfrak{f}_0'$. Then $\chi_{\mathfrak{p}}(\alpha) = \chi_{\mathfrak{p}}(\beta) \equiv \beta^{-k} \equiv \alpha^{-k} \bmod \mathfrak{p}$. Hence the relation $\chi_{\mathfrak{p}}(\alpha) \equiv \alpha^{-k} \bmod P$ holds for α prime to $\mathfrak{f}(\chi)$. Let $\chi' = \prod_{v|\mathfrak{f}_0'} \chi_v$. Then for α prime to $\mathfrak{f}(\chi)$, $\chi(C_{(\alpha)}) = \chi'(\alpha^{-1})\, \chi_{\mathfrak{p}}(\alpha^{-1})$. For α prime to $\mathfrak{f}_0'$, define

$$\tilde{\chi}((\alpha)) = \chi'(\alpha)\, \bar{\alpha}^k.$$

This is well defined. For, if $\varepsilon \in \mathfrak{o}^\times$, $\chi'(\varepsilon) = \chi_{\mathfrak{p}}(\varepsilon^{-1}) \equiv \varepsilon^k \bmod P$. Since $p \geqslant 5$, $\chi'(\varepsilon) = \varepsilon^k$, and $\chi'(\varepsilon)\,\bar{\varepsilon}^k = 1$. For α prime to $\mathfrak{f}(\chi)$, we see

$$\begin{aligned}\tilde{\chi}((\alpha)) &= \chi(C_{(\alpha)})^{-1}\chi_{\mathfrak{p}}(\alpha)^{-1}\,\bar{\alpha}^k \\ &\equiv \chi(C_{(\alpha)})^{-1}\,N\alpha^k \qquad \bmod P.\end{aligned}$$

Let $\mathscr{I}(\mathfrak{f}_0')$ be the group of all ideals prime to $\mathfrak{f}_0'$ and $\mathscr{P}(\mathfrak{f}_0')$ its subgroup consisting of principal ideals. Let $\mathscr{I}(\mathfrak{f}_0')/\mathscr{P}(\mathfrak{f}_0') \simeq Z_{n_1} \times \cdots \times Z_{n_s}$ for cyclic groups Z_{n_i} of order n_i. Then $\Pi_i n_i = h$ is prime to p. Choose $\mathfrak{a}_i$ so that $(\mathfrak{a}_i, \mathfrak{f}(\chi)) = (1)$ and $\mathfrak{a}_i$ generates Z_{n_i}. Let $\tilde{\chi}(\mathfrak{a}_i^{n_i})^{1/n_i}$ be the unique n_ith root of $\tilde{\chi}(\mathfrak{a}_i^{n_i})$ which satisfies

$$\tilde{\chi}(\mathfrak{a}_i^{n_i})^{1/n_i} \equiv \chi(C_{a_i})^{-1}\,N\mathfrak{a}_i^k \qquad \bmod P.$$

Define $\tilde{\chi}(\mathfrak{a}_i) = \tilde{\chi}(\mathfrak{a}_i^{n_i})^{1/n_i}$ and $\tilde{\chi}(\mathfrak{a}) = \tilde{\chi}((\alpha))\prod_i \tilde{\chi}(\mathfrak{a}_i)^{m_i}$ for $\mathfrak{a} = (\alpha)\prod_i \mathfrak{a}_i^{m_i}$. It is easy to see $\tilde{\chi}$ has the required properties. This completes the proof.

By the construction, the values of $\tilde{\chi}$ are contained in an extension of K which is unramified at p.

PROPOSITION 3.5. *Let τ_2 be as in Section 2. Assume $\chi \in X_{M/N}$ satisfies (3.2) for k, and let $\tilde{\chi}$ be as in Proposition 3.4. If $\chi \neq \omega_K$, $\tau_2^{-k} L(k, \tilde{\chi})$ is P-integral. If $\chi = \omega_K$, $\tilde{\omega}\tau_2^{-k} L(k, \tilde{\chi})$ is a P-unit.*

Proof. Let $\mathfrak{f}' = \mathfrak{f}(\chi)$, $\mathfrak{f}_0' = \mathfrak{f}'/\mathfrak{p}$, and $\tau_2^{-1}\mathscr{L}' = \mathfrak{f}_0'\mathfrak{c}^{-1}$ with $\mathfrak{c}$ prime to $\mathfrak{f}'$. Then

$$\begin{aligned}&\sum_{\mathfrak{a} \in I(\mathfrak{f}')} \tilde{\chi}(\mathfrak{a})\,N\mathfrak{a}^{-k} E_k(\tau_2, \mathfrak{a}^{-1}\mathscr{L}') \\ &\quad = w(\mathfrak{f}')^{-1}\, w(\mathfrak{f}_0')(N\mathfrak{p} - 1)\,\tilde{\chi}(\mathfrak{c}^{-1})\,N\mathfrak{c}^k \tau_2^{-k} L(k, \tilde{\chi}). \qquad (3.3)\end{aligned}$$

The following is P-integral:

$$\begin{aligned}&\sum_{\mathfrak{a} \in I(\mathfrak{f}')} \tilde{\chi}(\mathfrak{a})\,N\mathfrak{a}^{-k}(N\mathfrak{a} E_k(\tau_2, L') - E_k(\tau_2, \mathfrak{a}^{-1}\mathscr{L}')) \\ &\quad = \Bigg(\sum_{\mathfrak{a} \in I(\mathfrak{f}')} \tilde{\chi}(\mathfrak{a})\,N\mathfrak{a}^{1-k}\Bigg) E_k(\tau_2, \mathscr{L}') \\ &\qquad - \sum_{\mathfrak{a} \in I(\mathfrak{f}')} \tilde{\chi}(\mathfrak{a})\,N\mathfrak{a}^{-k} E_k(\tau_2, \mathfrak{a}^{-1}\mathscr{L}').\end{aligned}$$

If $\sum_{\mathfrak{a} \in I(\mathfrak{f}')} \tilde{\chi}(\mathfrak{a})\,N\mathfrak{a}^{1-k} \equiv 0 \bmod P$, our assertion follows from this. This is satisfied if $\chi \neq \omega_K$. If $\chi = \omega_K$, $\sum_{\mathfrak{a} \in I(\mathfrak{f}')} \chi(\mathfrak{a}^{-1})\,N\mathfrak{a} \equiv |I(\mathfrak{f}')| \bmod P$. In this case, $(|I(\mathfrak{f}')|, p) = 1$, and our assertion follow from this and Corollary 2.8.

Let $\bar{X}_M$ be the set of characters of G with values in $\bar{\mathbf{F}}_p$ as in Section 1 and

$X_{M/N}$ its subset consisting of χ such that $\operatorname{Ker}\chi \not\supset \operatorname{Gal}(M/N)$. Then the reduction modulo P gives rise to a bijection between X_M (resp. $X_{M/N}$) and $\bar{X}_M$ (resp. $\bar{X}_{M/N}$). We denote by $\bar{\chi}$ the image of $\chi \in X_M$.

In the rest of this section, we assume L contains the Hilbert class field H.

THEOREM 3.6. *Let $\psi, \chi \in X_{M/N}$, and assume $\bar{\psi}|_{G_T} = c_k|_{G_T}$. Let $\mathfrak{b}$ be an integral ideal prime to $\mathfrak{f}$ such that the image of $C_\mathfrak{b}$ in G/G_χ is g_χ. If $\psi \notin \hat{\chi}$, $\Phi_k(1_{\hat{\psi}}(\theta_{\hat{\chi}} \otimes 1)) \equiv 0$, $\Phi'_k(1_{\hat{\psi}}(\theta_{\hat{\chi}} \otimes 1)) \equiv 0 \bmod P$. If $\psi = \chi$, one has*

$$\Phi_k(1_{\hat{\chi}}(\theta_{\hat{\chi}} \otimes 1)) \equiv C_\chi (N\mathfrak{a}_\chi - \tilde{\chi}(a_\chi)^{-1} N\mathfrak{a}_\chi^k)\, \tau_2^{-k} L(k, \tilde{\chi}) \qquad \bmod P,$$

$$\Phi'_k(1_{\hat{\chi}}(\theta_{\hat{\chi}} \otimes 1)) \equiv (C_{\chi'}(N\mathfrak{a}_\chi - \tilde{\chi}'(\mathfrak{a}_\chi)^{-1} N\mathfrak{a}_\chi^{k(p)}) \times \tau_2^{-k(p)} L(k(p), \tilde{\chi}'))^p \qquad \bmod P,$$

where

$$C_\chi = 12(-1)^{k-1} w(\mathfrak{f}(\chi)/\mathfrak{p})\, w(\mathfrak{f}(\chi))^{-1} (N\mathfrak{p} - 1)\, r_\chi^{-1} \tilde{\chi}(\mathfrak{c})^{-1} N\mathfrak{c}^k \times \prod_{q | r_\chi} (1 - (\tilde{\chi}(\mathfrak{b})^{-1} N\mathfrak{b}^k)^{r_\chi/q}).$$

When p remains prime in K, χ' denotes the element of $X_{M/N}$ such that $\chi'^p = \chi$.

Proof. Let $\mathfrak{f}' = \mathfrak{f}(\chi)$ and $\mathfrak{f}'_0 = \mathfrak{f}'/\mathfrak{p}$. If $\operatorname{Ker}\chi \not\subset \operatorname{Ker}\psi$, it is easy to see $\Phi_k(1_{\hat{\psi}}(\theta_{\hat{\chi}} \otimes 1)) \equiv 0$ and $\Phi'_k(1_{\hat{\psi}}(\theta_{\hat{\chi}} \otimes 1)) \equiv 0$. Assume $\operatorname{Ker}\chi \subset \operatorname{Ker}\psi$. Let X_χ be the group generated by χ and I_χ the kernel of χ in $I(\mathfrak{f}')$. For a set S of prime numbers dividing r_χ, let $\mathfrak{b}(S) = \prod_{q \in S} \mathfrak{b}^{r_\chi/q}$ and let $\mathfrak{b}(S) = \mathfrak{o}$ if S is the empty set. Now we have

$$\theta_{\hat{\chi}}^{r_\chi} = \prod_{\mathfrak{l} \in I(\mathfrak{f}')} \theta(C'_0, \mathfrak{a}_\chi)^{((1, K(\mathfrak{f}')/K) \sum_{\eta \in X_\chi} \eta(C_\mathfrak{l}))\, D_{\hat{\mathfrak{l}}}}.$$

From this we see $\Phi_k(1_{\hat{\psi}}(\theta_{\hat{\chi}} \otimes 1)) \equiv 12(-1)^{k-1} r_\chi^{-2} V(\psi, \chi) \bmod P$, where

$$V(\psi, \chi) = \sum_{\substack{\eta \in X_\chi \\ \mathfrak{l} \in I(\mathfrak{f}') \\ \mathfrak{g} \in I(\mathfrak{f}')/I_\chi \\ S}} \eta(C_\mathfrak{l})\, \psi(C_\mathfrak{g})^{-1} \sum_S (-1)^{|S|} \times (N\mathfrak{a}_\chi E_k(\tau_2, (\mathfrak{lgb}(S))^{-1} \mathscr{L}') - E_k(\tau_2, (\mathfrak{a}_\chi \mathfrak{lgb}(S))^{-1} \mathscr{L}'))$$

$$= \sum_{\substack{\eta \in X_\chi \\ \mathfrak{g} \in I(\mathfrak{f}')/I_\chi}} \eta(C_\mathfrak{g})^{-1} \psi(C_\mathfrak{g})^{-1} \Bigg(\sum_{\mathfrak{l} \in I(\mathfrak{f}')} \sum_S (-1)^{|S|} \eta(C_\mathfrak{l}) \times (N\mathfrak{a}_\chi E_k(\tau_2, (\mathfrak{lb}(S))^{-1} \mathscr{L}') - E_k(\tau_2, (\mathfrak{a}_\chi \mathfrak{lb}(S))^{-1} \mathscr{L}')) \Bigg) \bmod P.$$

Hence $\Phi_k(1_{\hat\psi}(\theta_{\hat\chi}\otimes 1))$ vanishes unless $\psi\in X_\chi$. Let $\psi\in X_\chi$. We note $r_\psi | r_\chi/q$ for some $q|r_\chi$ if $\hat\psi\neq\hat\chi$. The assumption implies

$$\tilde\psi(C_{(\alpha)})\equiv\alpha^k \qquad \bmod P,$$

for α such that $(\alpha, \mathfrak{f}(\psi))=1$ and $\alpha\equiv 1 \bmod \mathfrak{f}(\psi)/\mathfrak{p}$ by Lemma 2.4. Let $\tilde\psi$ be the Grössencharacter as in Proposition 3.4. Then by (3.3) we have

$$\begin{aligned} V(\psi,\chi) &\equiv r_\chi \sum_{S,\mathfrak{l}} (-1)^{|S|}\tilde\psi(\mathfrak{l})\, N\mathfrak{l}^{-k}\,(N\mathfrak{a}_\chi E_k(\tau_2, (\mathfrak{l}\mathfrak{b}(S))^{-1}\mathscr{L}') \\ &\quad - E_k(\tau_2, (\mathfrak{a}_\chi\mathfrak{l}\mathfrak{b}(S))^{-1}\mathscr{L}')) \qquad \bmod P \\ &\equiv r_\chi\Big(\prod_{q|r_\chi}(1-(\tilde\psi(\mathfrak{b})^{-1}N\mathfrak{b}^k)^{r_\chi/q})\Big)(N\mathfrak{a}_\chi-\tilde\psi(\mathfrak{a}_\chi)^{-1}N\mathfrak{a}_\chi^k) \\ &\quad \times |I(\mathfrak{f}')/I(\mathfrak{f}(\tilde\chi))|\,\tilde\psi(\mathfrak{c})^{-1}N\mathfrak{c}^k\tau_2^{-k}L(k,\tilde\psi) \qquad \bmod P. \end{aligned}$$

The case of Φ_k' can be treated in the same way. This completes the proof.

We note C_χ and $C_{\chi'}$ are P-units and $(N\mathfrak{a}_\chi-\tilde\chi(\mathfrak{a}_\chi)^{-1}N\mathfrak{a}_\chi^k)$ is a P-unit if $\chi\neq\omega_K$.

COROLLARY 3.7. *Let l and ζ be as in Corollary* 2.8 *and its proof, and let $\chi=\omega_K$. Then $\Phi_l(1_{\tilde\chi}(\theta_{\tilde\chi}\otimes 1))\not\equiv 0 \bmod P$. If p remains prime in K, $\Phi_l'(1_{\tilde\chi}(\theta_{\tilde\chi}\otimes 1))\equiv(\Phi_l(1_{\tilde\chi}(\theta_{\tilde\chi}\otimes 1)))^p \bmod P$ and $\Phi_{\tilde\chi}(1_{\tilde\chi}(\theta_{\tilde\chi}\otimes 1))$ and $\Phi_{\tilde\chi}(1_{\tilde\chi}(\zeta\otimes 1))$ are linearly independent over $\bar{\mathbf{F}}_p$.*

Proof. For $\chi=\omega_K$, $N\alpha_\chi-\tilde\chi((\alpha_\chi))^{-1}N\alpha_\chi^l = N\alpha_\chi-\alpha_\chi^l$, hence $(N\alpha_\chi-\tilde\chi((\alpha_\chi))^{-1}N\alpha_\chi^l)/\tilde\omega$ is a P-unit. The first assertion follows from this and Proposition 3.5. Since $\chi'=\chi=\omega_K$, the second assertion is immediate. Since $\sqrt{D}^p\equiv-\sqrt{D} \bmod P$, by (2.2) and the proof of Proposition 3.5, we have

$$\begin{aligned} \Phi_{\tilde\chi}(1_{\tilde\chi}(\theta_{\tilde\chi}\otimes 1)) &\equiv 12(-1)^p C_\chi((N\alpha_\chi-\alpha_\chi^{p+1})/p)\,|I(\mathfrak{f}')| \\ &\quad\times(pE_{p+1}(\tau_2,\mathscr{L}'),(pE_{p+1}(\tau_2,\mathscr{L}'))^p) \qquad \bmod P, \\ \Phi_{\tilde\chi}(1_{\tilde\chi}(\zeta\otimes 1)) &\equiv 24N(\mathfrak{f}'/\mathfrak{p})\sqrt{D}\,(pE_{p+1}(\tau_2,\mathscr{L}'), \\ &\quad -(pE_{p+1}(\tau_2,\mathscr{L}'))^p) \qquad \bmod P. \end{aligned}$$

Since $pE_{p+1}(\tau_2,\mathscr{L}')\not\equiv 0 \bmod P$, this completes the proof.

COROLLARY 3.8. *Let $\tilde\chi|_{G_T}=c_k|_{G_T}$. If $k\in\mathscr{K}_2$ or $k(p)\in\mathscr{K}_2$,*

$$\tau_2^{-k}L(k,\tilde\chi)\equiv 0 \bmod P \Leftrightarrow \tau_2^{-k(p)}L(k(p),\tilde\chi')\equiv 0 \bmod P.$$

This follows immediately from Proposition 1.7 and Theorem 3.6.

4. A Kummer's Criterion

Let S and T be algebraic number fields such that $S \supset T \supset K$. We say S is $\mathfrak{p}$-ramified over T if S is unramified at all primes of T not dividing $\mathfrak{p}$. Let $\mathcal{M}_T$ be the maximal $\mathfrak{p}$-ramified p-abelian extension of T, and $\mathcal{M}_T^u$ be the maximal unramified p-abelian extension of T. Let $\mathcal{X}_T = \mathrm{Gal}(\mathcal{M}_T/M)$, $\mathcal{Y}_T = \mathrm{Gal}(\mathcal{M}_T^u/M)$ and let $\mathcal{Z}_T$ be the kernel of the restriction map of $\mathcal{X}_T$ onto $\mathcal{Y}_T$. If T is a Galois extension of K, $\mathcal{X}_T$, $\mathcal{Y}_T$ and $\mathcal{Z}_T$ are $\mathbf{Z}_p[\mathrm{Gal}(T/K)]$-modules by $x \mapsto \tilde{g}^{-1} x \tilde{g}$ for $x \in \mathcal{X}_T$, $\mathcal{Y}_T$ or $\mathcal{Z}_T$ and $g \in \mathrm{Gal}(T/K)$, where $\tilde{g}$ is an extension of g to $\mathrm{Gal}(\mathcal{M}_T/K)$.

Let L, M, N be as in Section 3. Let R be the restriction map of $\mathcal{X}_M$ into $\mathcal{X}_N$ and R' that of $\mathcal{Y}_M$ into $\mathcal{Y}_N$. Let j be the map of $\mathcal{X}_N$ into $\mathcal{X}_M$ induced by the natural injection $N_A^\times \to M_A^\times$ and j' that of Y_N into Y_M. Since $([M:N], p) = 1$, R and R' are surjective and j and j' are injective. Let $\mathcal{X}_{M/N} = \mathrm{Ker}\, R$, $\mathcal{Y}_{M/N} = \mathrm{Ker}\, R'$ and $\mathcal{Z}_{M/N} = \mathrm{Ker}\, R \cap \mathcal{Z}_M$. Then $\mathcal{X}_M = \mathcal{X}_{M/N} \oplus j(\mathcal{X}_N)$, $\mathcal{Y}_M = \mathcal{Y}_{M/N} \oplus j'(\mathcal{Y}_N)$ and $\mathcal{Z}_M = \mathcal{Z}_{M/N} \oplus j(\mathcal{Z}_N)$. Let $\mathcal{M}_{M/N}$ and $\mathcal{M}_{M/N}^u$ be the subfields of $\mathcal{M}_M$ and $\mathcal{M}_M^u$ corresponding to $j(\mathcal{X}_N)$ and $j'(\mathcal{Y}_N)$, respectively. Then $\mathcal{X}_{M/N} \simeq \mathrm{Gal}(\mathcal{M}_{M/N}/M)$ and $|\mathcal{Y}_{M/N}| =$ the p-part of $h_{M/N}$.

Let $U_{M/N}^{(1)}$ be the kernel of the norm map of $U_M^{(1)}$ to $U_N^{(1)}$. Let $E_{M/N}^{(1)} = E_{M/N} \cap U_M^{(1)}$ and let $\bar{E}_{M/N}$ be the closure of $E_{M/N}^{(1)}$ in $U_{M/N}^{(1)}$. Then $Z_{M/N} \simeq U_{M/N}^{(1)}/\bar{E}_{M/N}$ as $\mathbf{Z}_p[G]$-modules. Let $\bar{\Theta}_{M/N}$ be the closure of $(\Theta_{M/N}\mu_{M/N}) \cap E_{M/N}^{(1)}$ in $U_{M/N}^{(1)}$. Then $[\bar{E}_{M/N}: \bar{\Theta}_{M/N}]$ is equal to the p-part of $h_{M/N}$. Let $X_{M/N}^1$ be the set of $\chi \in X_{M/N}$ such that $\tilde{\chi}|_{G_T} = c_k|_{G_T}$ for $k \in \mathcal{H}_1$ and $\chi \neq \omega_K$, and let $X_{M/N}^2$ be the set of $\chi \in X_{M/N}$ such that $\tilde{\chi}|_{G_T} = c_k|_{G_T}$ for $k \in \mathcal{H}_2$ or $k(p) \in \mathcal{H}_2$. Then the union $X_{M/N} = X_{M/N}^1 \cup X_{M/N}^2 (\cup \omega_K)$ is disjoint. If p decomposes or ramifies in K, $X_{M/N}^2$ is empty, and we set $k(p) = k$ and $\chi' = \chi$. For $m = [M:L]$, let $\mathcal{F}(m)$ be the composite of all cyclic extensions of M of degree p in $\mathcal{M}_{M/N}$ whose conductors divide $\mathfrak{p} = (\mathfrak{P}_1 \cdots \mathfrak{P}_s)^m$.

THEOREM 4.1. *Let the notation be as above. Consider the following conditions*:

(A) $(\tau_2^{-k} L(k, \tilde{\chi}),\ \tau_2^{-k(p)} L(k(p), \tilde{\chi}')) \equiv 0 \bmod P$ *for some* $\chi \in X_{M/N}^1$;

(B) $\tau_2^{-k} L(k, \tilde{\chi}) \equiv 0 \bmod P$ *for some* $\chi \in X_{M/N}^2$;

(a) $h_{M/N}$ *is divisible by* p;

(b) $(h_{M/N}, p) = 1$ *and* $\mathcal{X}_{M/N}$ *has a torsion*;

(c) $(h_{M/N}, p) = 1$, $\mathcal{X}_{M/N}$ *is torsion-free and* $\dim_{\mathbf{F}_p} \mathrm{Gal}(\mathcal{F}(m)/M) > |X_{M/N}^1|$.

Then (A) *or* (B) *occurs if and only if* (a), (b) *or* (c) *occurs. Moreover,* (c) *implies that* p *remains prime and* (B) *or* p *ramifies and* (A).

Proof. First assume L contains H. Let $\tilde{\Theta}_{M/N}$, $\tilde{E}_{M/N}$ and $\tilde{U}_{M/N}$ be the image of $\bar{\Theta}_{M/N}$, $\bar{E}_{M/N}$ and $U^{(1)}_{M/N}$ in W. Let V be one of $\tilde{\Theta}_{M/N}$, $\tilde{E}_{M/N}$ and $\tilde{U}_{M/N}$. Then

$$V \otimes_{\mathbf{F}_p} \bar{\mathbf{F}}_p \simeq \bigoplus_{\chi \in X_{M/N}} V(\bar{\chi}).$$

We note $\tilde{U}_{M/N}(\bar{\chi}) = W(\bar{\chi})$ for $\chi \in X_{M/N}$. By Corollary 3.7, we have $\tilde{U}_{M/N}(\bar{\omega}_K) = \tilde{\Theta}_{M/N}(\bar{\omega}_K)$. Hence, by Theorem 3.6 and Corollary 3.8, the condition that (A) or (B) occurs is equivalent to that $\tilde{\Theta}_{M/N}(\chi)$ vanishes for some $\chi \in X_{M/N}$. Assume this. We prove (c) under the condition that neither (a) nor (b) holds. This implies $\bar{\Theta}_{M/N} = \bar{E}_{M/N}$ and $U^{(1)}_{M/N}/\bar{E}_{M/N}$ is torsion-free. Consider the natural map:

$$\lambda : U^{(1)}_{M/N}/U^{(1)p}_{M/N} U^{(m)}_{M/N} \to U^{(1)}_{M/N}/U^{(1)p}_{M/N} U^{(m)}_{M/N} \bar{E}_{M/N}.$$

Here $U^{(m)}_{M/N} = U^{(1)}_{M/N} \cap U^{(m)}_{M}$. The right-hand side is isomorphic to $\mathrm{Gal}(\mathscr{F}(m)/M)$. If $\tilde{E}_{M/N}(\bar{\chi}) = 0$ for some $\chi \in X_{M/N}$, p remains prime and χ is contained in $X^2_{M/N}$, or p ramifies, since $U^{(1)}_{M/N}/\bar{E}_{M/N}$ is torsion-free. Let δ be 1 or 0 according as $X_{M/N}$ contains ω_K or not. Then $\dim_{\mathbf{F}_p} \mathrm{Ker}\, \lambda < |X_{M/N}| + \delta$, hence $\dim_{\mathbf{F}_p} \mathrm{Gal}(\mathscr{F}(m)/M) > |X^1_{M/N}|$.

Conversely, it is easy to see (a) implies $\tilde{\Theta}_{M/N}(\bar{\chi}) = 0$ for some $\chi \in X_{M/N}$, since $[\bar{E}_{M/N} : \bar{\Theta}_{M/N}]$ is the p-part of $h_{M/N}$. Assume (b). Then $\dim_{\mathbf{F}_p} \tilde{E}_{M/N} < |X_{M/N}| + \delta$, hence $\tilde{E}_{M/N}(\bar{\chi}) = 0$ for some $\chi \in X_{M/N}$ and $\tilde{\Theta}_{M/N}(\bar{\chi}) = 0$ for some $\chi \in X_{M/N}$. As to (c) we see easily the condition $\dim_{\mathbf{F}_p} \mathrm{Gal}(\mathscr{F}(m)/M) > |X^1_{M/N}|$ implies $\tilde{E}(\bar{\chi}) = 0$ for some $\chi \in X_{M/N}$.

If L does not contain H, consider the fields $M' = MH$, $N' = NH$ and $L' = LH$. By considering $\mathrm{Gal}(M'/M)$-invariant subspaces, we see for $V = \tilde{U}$, $\tilde{E}$ or $\tilde{\Theta}$

$$V_{M/N} \otimes_{\mathbf{F}_p} \bar{\mathbf{F}}_p \simeq \oplus V_{M'/N'}(\bar{\chi}),$$

where the sum is taken over all $\chi \in X_{M'/N'}$ which are trivial on $\mathrm{Gal}(M'/M)$. By using this, we can proceed in the same way as above. This completes the proof.

REFERENCES

1. J. COATES AND A. WILES, Kummer's criterion for Hurwitz numbers, *in* "Algebraic Number Theory," pp. 9–23, papers contributed to the International Symposium, Kyoto, 1976, Japan Society for the Promotion of Science, Tokyo, 1977.
2. R. GILLARD, Séries d'Eisenstein et critère de Kummer, *in* "Seminaire de theorie de nombres, Paris 1981–2," Progress in Mathematics, Vol. 38, Birkhäuser, Boston/Basel/Stuttgart, 1983.

3. C. GOLDSTEIN AND N. SCHAPPACHER, Seriés d'Eisenstein et fonction L de coubes elliptiques à multiplication complexe, *J. Reine Angew. Math.* **327** (1981), 184–218.
4. H. HIDA, Kummer's criterion for the special values of Hecke L-functions of imaginary quadratic fields and congruences among cusp forms, *Invent. Math.* **66** (1982), 415–459.
5. H. ITO, Congruence relation of Ankeny–Artin–Chowla type for pure cubic fields, *Nagoya Math. J.* **96** (1984), 95–112.
6. K. IWASAWA, On Galois group of local fields, *Trans. Amer. Math. Soc.* **80** (1955), 448–469.
7. H. W. LEOPOLDT, Über Einheitengruppe und Klassenzahl reeller Zahlkörper, *Abh. Deutsch. Akad. Wiss. Berlin, Kl. Math. Nat.* 1953, No. 2 (1954).
8. K. RAMACHANDRA, Some applications of Kronecker's limit formula, *Ann. of Math.* **80** (1964), 104–148.
9. G. ROBERT, Unités elliptiques, *Bull. Soc. Math. France*, mémoire **36** (1973).
10. G. ROBERT, Nombres de Hurwitz et unités elliptiques, *Ann. Sci. École Norm. Sup.* (4) **II** (1978), 297–389.
11. C. L. SIEGEL, "Lectures on Advanced Analytic Number Theory," Tata Institute of Fundamental Research, Bombay, 1961.
12. G. SHIMURA, "Introduction to the Arithmetic Theory of Automorphic Functions," Publ. Math. Soc. Japan No. 11, Iwanami Shoten and Princeton Univ. Press, Tokyo/Princeton, N.J., 1971.
13. R. I. YAGER, A Kummer's criterion for imaginary quadratic fields, *Compositio Math.* **47** (1982), 31–42.